

## CLAIMS

What is claimed is:

1. A method for controlling input/output (I/O) operations of a user's computer comprising the following steps:
  1. implementing the user's computer as a virtual machine (VM);
    1. including a virtual machine monitor (VMM) as a VM-transparent interface
  2. between the VM and a physical computer system that includes at least one device;
    1. in the VMM:
      1. sensing a request for an I/O operation between the VM and the device;
      2. performing a predetermined transformation of I/O data passing between the VM and the device;
    2. the transformation of the I/O data thereby being undefeatable by any user action via the VM.
  2. A method as in claim 1, in which:
    1. the device is a display;
    2. the I/O data is VM display data output from the VM and intended for display; and
    3. the predetermined transformation is a replacement of at least a portion of the VM display data with non-defeatable display data stored external to the VM but accessible to the VMM;
    4. further including the step of displaying the VM display data with the non-defeatable display data overlaid.
  3. A method as in claim 1, further including the following steps:
    1. filtering the I/O data with respect to at least one predetermined filtering condition;
    2. and
    3. performing the predetermined transformation of the I/O data only when the filtering condition is met.

4. A method as in claim 3, in which the filtering condition is that the I/O data includes at least one predetermined restricted term.

5. A method as in claim 3, in which the filtering condition is that the I/O data is from a predetermined restricted source.

6. A method as in claim 3, in which:

the I/O data includes image data;

the step of filtering the I/O data comprises detecting the presence of a representation of a target image within the image data; and

5 the predetermined transformation is substitution of a representation of a replacement image in place of the representation of the target image.

7. A method as in claim 6, in which:

the I/O data is in a non-character image format;

the target image is a representation of a restricted character string; and

5 the step of filtering the I/O data comprises applying character recognition to the I/O data.

8. A method as in claim 3, in which the predetermined filtering condition is the presence in the I/O data of a copy protection indication.

9. A method as in claim 1, in which the predetermined transformation comprises insertion into the I/O data of a source indication associated with the VM.

10. A method as in claim 1, in which the transformation is time-varying.

11. A method as in claim 1, in which the device is a network connection device.

12. A method as in claim 11, in which the predetermined transformation is a bandwidth limiting of the I/O data being transferred between the VM and the network connection device.

13. A method as in claim 11, in which:  
the requested I/O operation is a transfer of the I/O data between the VM and the network connection device; and  
the predetermined transformation is a time delay of the transfer.

14. A method as in claim 11, in which:  
the requested I/O operation is a transfer of the I/O data from the VM to a first destination address via the network connection device;  
the predetermined transformation is a redirection of the I/O data to a second destination address different from the first.

15. A method as in claim 1, in which:  
the device is a display;  
the display renders data stored in a display map; and  
the step of performing the predetermined transformation comprises  
altering a selected portion of the display map.

16. A method as in claim 15, in which the step of altering the selected portion of the display data comprises substituting predetermined, non-defeatable display data for the selected portion.

17. A method as in claim 15, in which the step of altering the selected portion of the display data comprises changing all occurrences in the display map of a display color to a predetermined replacement color.

18. A method as in claim 1, in which:  
the device is a data storage device;  
the requested I/O operation is a transfer of data between the VM and the storage device; and  
5 the step of performing the predetermined transformation comprises changing at least a portion of the data during the transfer between the VM and the storage device.

19. A method as in claim 18, in which the step of performing the predetermined transformation of the I/O data comprises encrypting data written by the VM to the data storage device and decrypting data read from the data storage device by the VM.

20. A method as in claim 18, in which the step of performing the predetermined transformation of the I/O data comprises compressing data written by the VM to the data storage device and decompressing data read from the data storage device by the VM.

21. A method as in claim 1, in which:  
the device is a network connection device;  
the requested I/O operation is a transfer of data between the VM and the network connection device; and  
5 the step of performing the predetermined transformation comprises changing at least a portion of the data during the transfer between the VM and the network connection device.

22. A method as in claim 21, in which the step of performing the predetermined transformation of the I/O data comprises encrypting data written by the VM to the network connection device and decrypting data read from the network connection device by the VM.

23. A method as in claim 21, in which the step of performing the predetermined transformation of the I/O data comprises compressing data written by the VM to the network connection device and decompressing data read from the network connection device by the VM.

24. A method as in claim 1, in which the step of performing the predetermined transformation of the I/O data comprises cryptographic transformation of the I/O data.

25. A method as in claim 1, in which:

- the VM supports a plurality of I/O modes;
- the step of filtering is performed on I/O data corresponding to a first one of the plurality of I/O modes; and
- the predetermined transformation is applied to I/O data in a second one of the I/O modes when the I/O data in the first I/O mode satisfies the transformation-triggering criterion.

26. A method as in claim 25, in which the I/O modes include a video mode and an audio mode.

27. A method for controlling input/output (I/O) of a user's computer comprising the following steps:

- implementing the user's computer as a virtual machine (VM);
- including a virtual machine monitor (VMM) as a VM-transparent interface

5 between the VM and a physical computer system that includes at least one device that carries out an I/O operation on the basis of device control data;

- storing the device control data associated with the VM in a buffer in the VMM;
- upon sensing a transformation command from an administrative system external to the VM, entering replacement data into at least a portion of the buffer;

10 the entry of the replacement data thereby being undefeatable by any user action via the VM.

28. A system for controlling input/output (I/O) operations of a user's computer, comprising:

- a virtual machine (VM) constituting the user's computer;
- a virtual machine monitor (VMM) forming a VM-transparent interface between

5 the VM and a physical computer system that includes at least one device;

- the VMM including means:
- for sensing a request for an I/O operation between the VM and the device;

10 and

- for performing a predetermined transformation of I/O data passing between the VM and the device;
- the transformation of the I/O data thereby being undefeatable by any user action via the VM.

29. A system as in claim 28, in which the device is a display and the I/O data is VM display data.

30. A system as in claim 29, further comprising:

a display buffer within the VMM for storing the VM display data that is output from the VM and is intended for display; and

5 transformation means located within the VMM for replacing at least a portion of the VM display data stored in the display buffer with non-defeatable display data; in which the display is provided for displaying the contents of the display buffer.

31. A system as in claim 28, in which the device is a data storage device.

32. A system as in claim 28, in which the device is a network connection device.